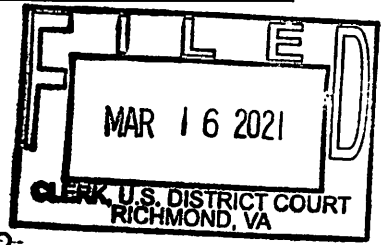


AO 106A (EDVA Version) (03/20) Application for a Warrant by Telephone or Other Reliable Electronic Means

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH APPLE ID  
omarimason1998@gmail.com THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case No. 3:21-sw-28

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated by reference herein.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute Controlled Substances
18 U.S.C. § 922(g)	Possession of a Firearm by a Convicted Felon

The application is based on these facts:

See Affidavit, incorporated by reference herein.

- ☐ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

David Dean

Applicant's signature

Reviewed by AUSA/SAUSA

Kenneth R. Simon, Jr.

Printed name and title

D.A. Dean, ATF Task Force Officer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
(specify reliable electronic means).

Date: 3/16/21

City and state: Richmond, Virginia

Elizabeth W. Hanes  
United States Magistrate Judge  
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
APPLE ID omarimason1998@gmail.com  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case No. 3:21sw 28

Under Seal

**AFFIDAVIT IN SUPPORT OF**

**AN APPLICATION FOR A SEARCH WARRANT**

I, David A Dean, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the Apple ID omarimason1998@gmail.com (hereinafter the “**SUBJECT ACCOUNT**”), that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California.. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Task Force Officer (TFO) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since September 2019. My law enforcement and legal training began in 2014 with the Chesterfield County Sheriff’s Office. In 2015, I started my career with Petersburg Bureau of Police as a Patrol Officer. While employed by the Petersburg Bureau of Police, I was transferred to the Special investigations Unit as a Detective. I received

specialized training in narcotics trafficking, gangs and violent crimes. In September 2019, I was transferred to the ATF as a TFO and assigned to the Richmond, Virginia Field Office. With my training knowledge and experience, I have discovered that narcotics traffickers utilize social media through the use of mobile devices to contact other individuals regarding their crimes, including the selling and potential selling of illegal narcotics. Such platforms of social media include, but are not limited to, Facebook, Twitter and Instagram.

3. I have come to understand that individuals use multiple platforms to access social media which include but are not limited to: cell phones, tablets, personal computers and video gaming consoles. I have come to understand that many individuals' use social media to contact others regarding crimes they have committed and/or crimes that they plan to commit.

4. During my tenure as a Detective and TFO, I have participated in, and led numerous investigations, to include but not limited to: homicide, organized crime, narcotics and firearms trafficking, and federal firearms violations. These violations are included in Title 18 and 21 of the United States Code. I have authored numerous search and seizure affidavits in connection with these investigations.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violation of 21 U.S.C § 841 (a) (1) manufacturing or possessing with intent to distribute a controlled substance and 18 U.S.C. § 922(g) possession of a firearm by a convicted felon have been committed by Omari Mason. There is also probable

cause to search the information described in Attachment A for evidence, contraband, instrumentalities, and fruits of these crimes further described in Attachment B.

### **JURISDICTION**

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

#### **A. Use of Phones by Narcotics Traffickers to Further their Criminal Activity**

8. Based on my training and experience, I know that it is common for individuals engaged in illegal trafficking of narcotics to use telephonic communications to further their criminal activities by coordinating the trafficking of narcotics, moving illegal proceeds of narcotics trafficking, and discussing other efforts of co-conspirators.

9. Based on my training and experience, I know that individuals engaging in the trafficking of narcotics use cellular telephones and cellular telephone technology to communicate and remain in constant contact with customers.

10. Based on my training and experience, I know that individuals who engage in the trafficking of narcotics use cellular telephones to exchange information with customers and/or source(s) of supply through text messaging, instant messaging, and direct telephone conversations.

11. Based on my training and experience, I know that cellular telephones are important to a criminal investigation of the distribution of illegal narcotics. In particular, I know:

a. that narcotic traffickers often use cellular telephones to communicate with sources of supply, drug transporters, facilitators, and customers in connection with their ongoing drug activities, including communication by live conversations, voice messages, text messages, emails, and similar communication methods all conducted via the cellular telephones that often have internet capabilities;

b. that narcotic traffickers often use cellular telephones to maintain records, contact information, notes, ledgers, and other records relating to the transportation, ordering, sale, and distribution of controlled substances, even though such documents may be in code. That the aforementioned books, records, notes, ledgers, etc., are commonly maintained where narcotic traffickers have ready access to them, including but not limited to their cellular telephones;

c. that narcotic traffickers commonly maintain names, addresses and telephone numbers in their cellular telephones for their associates in the narcotic trafficking organization, even if said items may be in code, and that these types of records are sometimes maintained in computers or other electronic data storage devices; and

d. that many cellular telephones have extensive photography and video capabilities. That many narcotic traffickers frequently use their cellular telephones to take, cause to be taken, photographs and/or videos of themselves, their co-conspirators and associates, their property, including firearms, and their product, and that these traffickers usually maintain these photographs and/or videos, on their cellular telephones

12. Based on my training and experience, I know that individuals who engage in the trafficking of narcotics often possess firearms to protect themselves and their narcotics. I have

debriefed confidential informants, interviewed narcotic traffickers and watched undercover video recordings of narcotic transactions that confirm this nexus.

B. Case Background

13. In the fall of 2019, Mason was released from the Virginia Department of Corrections after receiving a sentence in 2018 for possession of a firearm by a non-violent felon. The signed plea agreement entered between the Commonwealth of Virginia and Mason show that he agreed to a term of two years incarceration on the firearm possession offense and acknowledged that he could no longer possess a firearm.

14. On June 15, 2020, law enforcement searched a hotel room belonging to Omari MASON("Mason") and his girlfriend and located large amounts marijuana in a drawer with MASON's belongings, including clothing, a Smith and Wesson MP40, .40 caliber semi-automatic pistol, bearing Serial Number LET2178 that was located under the mattress, a digital scale containing white residue, and \$2844.00 in United States currency. The charges related to the items recovered as a result of this search remain pending. MASON's girlfriend stated that the items did not belong to her and indicated that she did not allow anyone other than MASON into the room.

15. On August 19, 2020, your Affiant responded to 13071 Pete Lane, Stony Creek, Virginia to assist with the location of wanted subject Mason. The residence was determined to belong to Alice Crowder ("Crowder"), MASON's girlfriend's grandmother. Ms. Crowder was present at the residence. While on scene, your Affiant was advised by USMS TFO Matthew Norman that USMS TFOs located MASON inside the residence.

16. While searching for Mason, USMS TFO Matthew Norman located suspected illegal narcotics inside a bedroom ("Bedroom One") in the residence. Your affiant was advised

by TFO Norman that, inside Bedroom One, he observed a fanny pack in plain view on the floor with the small zipper unzipped. Ms. Crowder advised that MASON was in the room where the fanny pack was located.

17. Moreover, TFO Norman heard commotion from Bedroom One after everyone except MASON had exited the residence. MASON was the only one remaining inside the residence. In Bedroom One, TFO Norman observed what appeared to be plastic baggies containing white and grayish powder sticking out of the unzipped pouch of the fanny pack. Moreover, TFO Norman advised that, based on his training and experience which includes multiple arrests involving narcotics trafficking, he concluded that the substance in the baggies were consistent with illegal narcotics.

18. It should be noted that Ms. Crowder was sitting outside on the lawn in a chair free to leave and was not under detention. At this time, your Affiant approached Ms. Crowder and asked her if he could speak with her alone. Ms. Crowder agreed to speak with your Affiant and, upon her request, your Affiant along with USMS TFO Norman assisted her back into the residence.

19. While inside the residence, your Affiant conducted an audio and video recorded interview of Ms. Crowder. Ms. Crowder was advised that USMS TFOs located what appeared to be illegal narcotics inside the residence. Your Affiant then asked her for consent to search the residence. Ms. Crowder advised your Affiant that it was her home and that she paid the bills. Ms. Crowder advised her highest level of education was fifth grade. Your Affiant then read the consent to search form to Ms. Crowder and advised her that he would only search the room with the drugs and the room that MASON ran into (her room). Ms. Crowder asked your Affiant if she could look to see which rooms your Affiant sought consent to search. Accordingly, your Affiant

along with TFO Norman walked her to the back rooms and showed her both rooms that they sought to search. Crowder then signed the consent form and allowed your Affiant to search both rooms.

20. Your Affiant started his search with Bedroom One—the bedroom where MASON had been heard as referenced in paragraph 17. Ms. Crowder stated that MASON was using the room. It should be reiterated that TFO Norman heard movement coming from Bedroom One after all other individuals exited the residence. Your affiant understood Ms. Crowder to mean that MASON was using the room on August 19, 2020. Ms. Crowder did, however, indicate that MASON arrived on August 18, 2020, left that evening, and returned again on August 19, 2020.

21. The items in Bedroom One included men's shoes and clothing piled up in the corner. These items matched MASON's build. In addition, of the individuals in the house, the only other males were adolescents who were much larger than Mason. The clothing did not appear to match the adolescent's build. Lastly, when MASON requested that TFO Norman grab his "grills" for MASON's teeth, MASON directed TFO Norman to the couch in bedroom one. "Grills" are metal plates that go over one's teeth.

22. During the search of bedroom one, your Affiant located a Hershel brand gray in color Fanny Pack on the floor beside a couch located in bedroom one. The Fanny Pack contained a Glock .40 caliber semi-automatic pistol, large amount of suspected heroin, cocaine, marijuana, a digital scale, pink lighter key chain, keys to a Cadillac vehicle, 2 gold chains, and a debit card bearing MASON's name. Your affiant also located a cellular telephone on the couch in bedroom one along with several other cellular devices. When shown a photograph of the fanny pack recovered from Bedroom One, MASON's girlfriend confirmed that MASON had a similar looking fanny pack when they were together on August 18, 2020.



23. Moreover, Mason's girlfriend identified Mason as the individual wearing a similar looking fanny pack in a photo posted on the Osama Loco account on August 9, 2020. Although the denominations are unclear, photographs of Mason posted to the Osama Loco account in May 2020, June 2020, and July 2020 appear to show Mason holding large sums of United States currency. A review of wages from the Virginia Employment Commission shows no reportable income for Mason throughout 2020.

24. Your affiant made contact with a Confidential Reliable Informant who advised he/she used cellphone number 804-605-7249 to contact MASON approximately three to four times per week throughout 2020. Through further investigation it was revealed that the IMEI number registered to phone number 804-605-7249 is 356432109485040. TFO Norman recovered the device with the **SUBJECT ACCOUNT** on the couch in bedroom one. That device has an IMEI number of 356432109485040.

25. On September 11, 2020, your Affiant sought and obtained a federal search warrant for one of the other devices located on the couch in Bedroom One, specifically a Motorola XT2005-4 bearing MEID 35217710162885. MASON's girlfriend stated that the Motorola was MASON's phone. Your Affiant reviewed the cellular telephone information for the Motorola XT2005-4. The information showed that the Motorola device (that MASON's girlfriend claimed belonged to MASON) was instead being used to contact MASON's girlfriend, leading your affiant to believe that MASON's girlfriend had misled law enforcement. Specifically, a review of that Motorola device revealed that, in fact, MASON had been contacting MASON's girlfriend on the Motorola XT2005-4 bearing MEID 35217710162885 using the cellular telephone number assigned to the device connected to the **SUBJECT ACCOUNT**.

26. On August 20, 2020, your Affiant conducted an open source review of Facebook page for an individual who uses the name “Osama Loco.” Your Affiant has come to know Facebook page Osama Loco is owned and operated by Omari Mason. While reviewing the Facebook page for Osama Loco, your Affiant observed multiple photos of MASON with a gray in color Hershel fanny pack along with a pink lighter key chain. Mason’s girlfriend stated that these were photos of MASON and that the fanny pack appeared the same as the one she had seen him with on August 18, 2020. TFO Dean also observed a Facebook photo of MASON with a gold chain containing a \$100 medallion that appeared to be the same medallion recovered from the fanny pack on August 19, 2020. Both the \$100 medallion and fanny pack from Facebook appear similar to the ones recovered from bedroom one on August 19, 2020.

27. On April 28, 2020, ATF Special Agent Adam Ulery obtained a Facebook search warrant for Facebook page Osama Loco, a Facebook page known to be operated by MASON. After executing the Facebook search warrant, S/A Ulery reviewed the returned content of the search warrant. S/A Ulery observed multiple private messages between MASON and multiple subjects who expressed an interest in purchasing controlled substances such as Xanax pills, Percocet pills, heroin, and marijuana from MASON between December 4, 2020 through April 4, 2021.

28. A review of the Osama Loco Facebook also revealed multiple messages and videos demonstrating Mason’s firearms possession. For example, the Osama Loco account responded to another user with, “I want it” when presented with a semi-automatic rifle offered for sale at \$650. Additionally, a recorded video by MASON from November 2019 shows him with what appears to be a handgun sticking out of the left side of MASON’s waistband in the video. A video recorded in December 2019, shows Mason holding what appears to be a handgun equipped with an extended

magazine. Mason is waving the handgun around while holding it by the extended magazine. Lastly, Mason's girlfriend stated that she has seen him with handguns in the past.

29. On September 29, 2020 your affiant obtained a search warrant for cell phone number 804-605-7249 with IMEI number 356432109485040. Your affiant then received the phone extraction data from the Virginia State Police for this phone. On the same day, a preservation letter was sent to Apple for any accounts associated with cell phone number 804-605-7249 with IMEI number 356432109485040. Furthermore, on October 6, 2020 your affiant sent a subpoena to Apple, Inc. requesting information associated with cell phone number 804-605-7249 with IMEI number 356432109485040.

30. On October 27, 2020 your affiant received a subpoena return from Apple, Inc. indicating that omarimason1998@gmail.com is the iCloud account associated with cell phone number 804-605-7249 with IMEI number 356432109485040. The return also show that the iCloud account was created on June 1, 2020 on the device connected to the **SUBJECT ACCOUNT**.

31. When executing the search warrant on the device connected to the **SUBJECT ACCOUNT**, the data showed that the information on the cell phone itself had been deleted. It also show that the iCloud account associated with the cell phone is omarimason1998@gmail.com.

32. Based on the information detailed in this affidavit, I submit that there is probable cause to believe that **Omari MASON** has used the **SUBJECT ACCOUNT** on his Apple iPhone to coordinate the illegal distribution of controlled substances. In addition, there is probable cause to believe that Mason has committed violations of possession of a firearm by a convicted felon, in violation of 18 U.S.C. § 922(g), and that the **SUBJECT ACCOUNT** will contain evidence, contraband, and property used in committing these crimes. I believe that information relevant to

the described unlawful activities by **Omari MASON** and his coconspirators, such as geolocation and other information pertaining to the unlawful sale of narcotics, are stored in the **SUBJECT ACCOUNT**. The **SUBJECT ACCOUNT** also may contain evidence of text messages, calls made and received, telephone numbers, contact names, electronic mail (email) addresses, appointment dates, pictures and other digital information, and such information may provide evidence of known illegal narcotics and firearms purchases and sales, and reveal other unknown illegal narcotics and firearms purchases and sales.

33. I know that Apple iPhones can back up communication data to the Apple iCloud account utilized by the user of the phone. I submit that original data stored within the **SUBJECT ACCOUNT** may contain other information previously deleted by **Omari Mason**. I, therefore, submit that there is probable cause to believe that iMessages, photographs, and other evidence as detailed in Attachment B are stored on **Omari MASON's** iCloud account.

#### **BACKGROUND CONCERNING APPLE<sup>1</sup>**

34. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

35. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>;

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

---

“Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

36. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email

addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

37. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

38. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

39. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial

number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

40. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some



of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

41. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of narcotics trafficking offenses, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of narcotics trafficking, including to communicate and facilitate the sale of narcotics.

43. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

### **CONCLUSION**

47. Based on the forgoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant

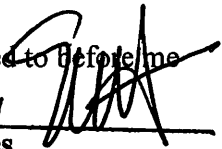
by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

*David Dean*

---

D.A. Dean  
Task Force Officer  
Bureau of Alcohol, Tobacco, Firearms and  
Explosives

Sworn and subscribed to before me

/s/   
Elizabeth W. Hanes  
United States Magistrate Judge

---

The Honorable Elizabeth W. Hanes  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with omarimason1998@gmail.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple Inc. (“Apple”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 29, 2020, Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from June 1, 2020 to August 19, 2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from June 1, 2020 to August 19, 2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 922(g), 21 U.S.C § 841 (a)(1), or 2 involving Omari MASON and his coconspirators and relate to violations of Title 18, United States Code, Section 922(g), 21 U.S.C § 841 (a)(1), or 2, including information pertaining to the following matters:

- a. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- b. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- c. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- d. The identity of the person(s) who communicated with the user ID about matters relating to narcotics trafficking, including records that help reveal their whereabouts;
- e. Incoming/outgoing/missed phone call logs;
- f. voicemail messages;
- g. Any photographs or videos of firearms, narcotics, narcotic related receipts, and documentation related to the purchase or sale of illegal narcotics;
- h. Records and information relating to any purchase or sale of firearms or illegal narcotics;
- i. lists of customers and related identifying information (contact list);



- j. Text messages, iMessages and messages on other Applications between **Omari MASON** and other co-conspirators concerning the transfer and/or sale of narcotics or firearms
- k. Records and information relating to the identity of co-conspirators, criminal associates, or others involved in the purchase or sale of illegal narcotics (including names, addresses, phone numbers, or any other identifying information);
- l. Records and information relating to geographic location of devices associated with the account, including travel to or from or presence at locations where illegal narcotics were purchased or sold;
- m. Calendar entries;
- n. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- o. Records and information that place in context, identify the creator or recipient of, or establish the time of creation or receipt of communications, records, or data involved in the activities described above;
- p. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- q. Evidence that may identify assets purchased with proceeds of narcotics sales

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC**  
**BUSINESS RECORDS PURSUANT TO FEDERAL RULE**  
**OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is \_\_\_\_\_. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes) associated with Apple ID omarimason1998@gmail.com. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and
- c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature